Propuesta de Tesis

Título: Soberanía Digital en el Marco del GDPR: Análisis Forense de Aplicaciones APK y Registros de Actividad

Autor: [Nombre del autor]
Tutor: [Nombre del tutor]
Programa: Maestría en Derecho Informático / Ciberseguridad y Análisis Forense Digital

1. Introducción

La ubicuidad de los dispositivos móviles ha desplazado el eje de la soberanía digital hacia el control que el usuario ejerce sobre los datos personales procesados en entornos de aplicaciones. Dicho control se ve frecuentemente comprometido por arquitecturas de almacenamiento opacas, diseñadas bajo lógicas de telemetría que operan al margen de la supervisión del titular de los datos. Esta tensión se agudiza cuando las técnicas de análisis forense digital — necesarias para la auditoría y la recuperación de evidencia — confrontan los estrictos límites de privacidad impuestos por el Reglamento General de Protección de Datos. La presente investigación busca conciliar la necesidad técnica de obtener información granular con los derechos fundamentales a la autodeterminación informativa del sujeto de datos.

La investigación se justifica ante la imperativa necesidad de establecer protocolos forenses que garanticen la integridad de la evidencia sin vulnerar la soberanía del usuario frente a agentes externos. Como punto de partida empírico, el estudio se apoya en la auditoría forense ejecutada sobre un dispositivo Samsung SM-A055M operando bajo Android 15, en el marco del Caso 3V3DJPD5 (Bentancor, n.d.). Este caso constituye un laboratorio natural para examinar cómo las plataformas de entretenimiento masivo actúan como vectores de exfiltración donde las protecciones nativas del kernel pueden ser neutralizadas mediante la inyección de SDKs de terceros (Bentancor, n.d.).

Pregunta de investigación: ¿Puede la estandarización de metodologías de extracción de datos en sistemas operativos móviles servir como salvaguarda ante la exfiltración arbitraria de información por parte de terceros, sin transgredir los límites del GDPR?

Objetivo general: Proponer un marco normativo-técnico que armonice los estándares de extracción forense con los principios de minimización de datos y limitación de la finalidad consagrados en el GDPR.

Objetivos específicos:

Analizar la estructura técnica de los archivos APK y los registros de actividad (logs) como

fuentes de evidencia forense.

Delimitar el alcance de la licitud probatoria, distinguiendo entre la recuperación técnica de registros de actividad y la recolección de datos personales que excede el propósito legítimo de la auditoría.

Evaluar el impacto de las transferencias internacionales de datos en la soberanía digital del usuario.

Formular recomendaciones institucionales para la auditoría de aplicaciones bajo criterios de confidencialidad y minimización.

La hipótesis central sostiene que la convergencia interdisciplinaria entre el análisis forense y el derecho de protección de datos permite auditar la infraestructura técnica de las aplicaciones — diseñada bajo lógicas de opacidad — asegurando el cumplimiento normativo frente a proveedores de servicios extracomunitarios, y reduciendo la asimetría informativa que dificulta el control efectivo de los usuarios sobre el tratamiento y las transferencias transfronterizas de sus datos personales.

2. Marco Legal

2.1 Principios de Protección

El GDPR estructura el tratamiento de datos sobre un conjunto de principios que operan como límites materiales a cualquier actividad de procesamiento. El principio de exactitud (Art. 5(d)) resulta de particular relevancia forense, pues la alteración no autorizada de datos personales constituye una infracción autónoma invocable ante la autoridad de control (“Gmail - ICO REFERRAL - Criminal Evidence ticket #2691688 - Roberto + Melisa - 24H DEADLINE.PDF,” n.d.). Asimismo, los principios de minimización de datos y limitación de la finalidad exigen que la recolección se restrinja a lo estrictamente necesario para el propósito declarado — estándar que debe gobernar también la actividad pericial, evitando que la extracción forense se convierta en un instrumento de vigilancia adicional.

2.2 Bases Jurídicas y Privacidad por Diseño

La licitud del tratamiento depende de la existencia de una base jurídica válida, siendo el consentimiento la más frecuentemente invocada en entornos de aplicaciones. La auditoría del Caso 3V3DJPD5 revela una contradicción técnica con grave responsabilidad legal: mientras la variable de recolección se encontraba habilitada (data_collection_enable: true), el campo de cumplimiento GDPR aparecía vacío («»), configurando una recolección forzada

sin consentimiento y una violación del principio de privacidad por diseño (Bentancor, n.d.). Este hallazgo demuestra que la exfiltración no siempre es accidental, sino que puede constituir una imposición técnica que vincula la identidad del usuario con sus privilegios de sistema (Bentancor, n.d.).

2.3 Derechos del Titular

El marco normativo otorga al titular derechos cuyo ejercicio resulta central en la disputa por la soberanía de sus datos. El derecho de acceso y la prohibición de decisiones automatizadas sin intervención humana fueron invocados en el caso de referencia ante el bloqueo del Oficial de Protección de Datos y la operación de soportes técnicos estructurados como «cajas negras» que impedían el ejercicio de la soberanía digital (Bentancor, n.d.). La exigencia de mediación humana frente a los muros algorítmicos constituye, en esta línea, uno de los ejes de la resistencia del usuario frente a la opacidad corporativa ("El Cáncer de la Memoria: La Autopsia del Caballo de Troya y la Batalla por la Soberanía Digital," 2026).

2.4 Alcance Territorial y Sanciones

El Reglamento posee alcance extraterritorial: el Art. 3 GDPR obliga a empresas extracomunitarias a cumplir con cualquier ciudadano cuyos datos sean tratados en el marco de sus actividades ("Gmail - ICO REFERRAL - Criminal Evidence ticket #2691688 - Roberto + Melisa - 24H DEADLINE.PDF," n.d.). Este principio habilita la interposición de denuncias ante autoridades de control como la ICO del Reino Unido, bajo la amenaza de las sanciones del Art. 83 ("Gmail - ICO REFERRAL - Criminal Evidence ticket #2691688 - Roberto + Melisa - 24H DEADLINE.PDF," n.d.). La dimensión sancionatoria refuerza la función disuasoria del régimen y constituye el respaldo institucional de los reclamos derivados de la exfiltración no consentida.

2.5 Transferencias Internacionales

En el plano de las transferencias transfronterizas, la infraestructura de las aplicaciones analizadas revela una topología distribuida entre nodos como AppLovin, AWS y Google Firebase/Google Cloud, con servidores ubicados — en el caso de Google — en Virginia (Bentancor, n.d.). Dicha configuración somete los datos de usuarios latinoamericanos y europeos a jurisdicciones extracomunitarias, agudizando la asimetría informativa y exigiendo mecanismos de garantía adicionales (cláusulas contractuales tipo, decisiones de adecuación o evaluación de impacto) para preservar la soberanía del titular.

3. Análisis Forense (APK/Logs)

3.1 Metodología de Extracción y Verificación de Integridad

El análisis forense de aplicaciones móviles requiere un procedimiento reproducible que garantice la inmutabilidad de la evidencia. En el caso de referencia se documentaron los activos analizados mediante la triple hash: MD5, SHA-1 y SHA-256 por paquete, incluyendo

identificadores como com.firsttouchgames.dls y com.multibox.clone.hub (Bentancor, n.d.). La verificación de integridad detectó una anomalía técnica en el SHA-1 de com.multibox.clone.hub (39 caracteres), lo que sugiere una inconsistencia en la cadena de metadatos o una truncación en el registro de origen — hallazgo relevante para evaluar la solidez de la cadena de custodia (Bentancor, n.d.). La firma de integridad del compendio (DLS7-AUDIT-2026-AB) consolidó la evidencia bajo referencias MD5 y SHA-256 verificables (Bentancor, n.d.).

3.2 Validación de Binarios y Detección de Repackaging

La validación de firmas digitales constituye el control primario para detectar procesos de repackaging — técnica que permite a actores externos inyectar código malicioso o ganchos de rastreo en binarios legítimos, facilitando la exfiltración silenciosa (Bentancor, n.d.). Este control es decisivo para verificar si el ecosistema analizado ha degradado la soberanía de los datos del usuario en favor de una infraestructura de inteligencia comercial (Bentancor, n.d.).

3.3 Triage de Permisos y Matriz de Riesgos

El examen del manifest.json (build 13130, min_sdk 36) reveló una aplicación que exige más de 15 permisos distintos, una extensión de privilegios que excede con creces la simulación deportiva (“EL CÁNCER DE LA MEMORIA Y LA RESISTENCIA DIGITAL,” 2024). La matriz de riesgos distingue entre permisos de riesgo operativo (INTERNET, VIBRATE, WAKE_LOCK), de sincronización (FOREGROUND_SERVICE_DATA_SYNC) e invasión crítica: USE_BIOMETRIC, USE_FINGERPRINT y ACCESS_ADSERVICES_AD_ID, que otorgan acceso directo a identificadores inmutables y perfiles publicitarios persistentes (“EL CÁNCER DE LA MEMORIA Y LA RESISTENCIA DIGITAL,” 2024). La pregunta forense es contundente: ¿por qué un simulador deportivo exige acceso a sensores biométricos, si la biometría es inmutable y vincula la huella dactilar a un perfil publicitario conlleva un riesgo permanente? (Bentancor, n.d.; “EL CÁNCER DE LA MEMORIA Y LA RESISTENCIA DIGITAL,” 2024)

3.4 Inyección de SDKs de Terceros

La aplicación no constituye un bloque monolítico: contiene «ganchos» (hooks) inyectados que no pertenecen al desarrollador original y operan con los mismos privilegios críticos (“EL CÁNCER DE LA MEMORIA Y LA RESISTENCIA DIGITAL,” 2024). El permiso BIND_APPHUB_SERVICE permite al SDK de AppLovin/AppHub operar como un servicio autónomo, rastreando al usuario a través de múltiples aplicaciones para construir un perfil de comportamiento independiente (“EL CÁNCER DE LA MEMORIA Y LA RESISTENCIA DIGITAL,” 2024). Esta arquitectura de telemetría oculta constituye la «caja negra» del sistema: el 80% de la exfiltración de datos sensibles no ocurre en el código del juego, sino en registros ocultos como array_hub_2026_04_14_12_44_43_643.log (“EL CÁNCER DE LA MEMORIA Y LA RESISTENCIA DIGITAL,” 2024).

3.5 Interpretación de Registros de Actividad

Los registros de depuración persistentes en formato JSON constituyen la fuente primaria de

evidencia de actividad (Bentancor, n.d.). Su interpretación revela prácticas de device fingerprinting: la captura de especificaciones exactas de hardware (SoC Mediatek MT6769V/WY, GPU Mali-G52) asegura que el usuario sea rastreable y monetizable incluso si restablece su ID de publicidad o reinstala la aplicación (“EL CÁNCER DE LA MEMORIA Y LA RESISTENCIA DIGITAL,” 2024). Los metadatos críticos detectados — IDFA, Device ID, operador (Claro UY / Uruguay), velocidad de red (30,000 kbps) y el estado data_collection_enable: true — configuran un patrón de recolección que excede cualquier necesidad operativa razonable (Bentancor, n.d.).

3.6 Cadena de Custodia y Licitud Probatoria

La cadena de custodia exige documentar cada transferencia de la evidencia: desde la extracción del archivo raíz (profile.dat, 34.01 KB, mayo de 2022, hash MD5 0995be55e79f7f94ca17a794d6898254) hasta su análisis y preservación (Bentancor, n.d.). El diseño metodológico debe establecer una distinción crítica entre la recuperación técnica de registros de actividad y la recolección de datos personales que exceden el propósito legítimo de la auditoría. En esta línea, el tratamiento de la evidencia pericial debe someterse a los mismos criterios de confidencialidad que rigen la evaluación de documentos reservados: no divulgar por ningún medio el material obtenido ni hacer uso de su contenido más allá del fin autorizado (“revisores_confidencialidad.pdf,” n.d.). La licitud probatoria depende, por tanto, de la proporcionalidad de la extracción y de la preservación de la soberanía del titular durante todo el proceso.

4. Conclusiones sobre Soberanía Digital

La evidencia analizada confirma que la soberanía digital no es una categoría abstracta, sino una capacidad concreta de control que se materializa en la documentación técnica, la verificación de integridad y el ejercicio efectivo de los derechos reconocidos en el GDPR. El caso de referencia demuestra cómo la precisión técnica transformó la reclamación individual en una «jurisprudencia de facto», obligando a la empresa a restaurar la verdad ante la evidencia de su propia vigilancia (Bentancor, n.d.). Esta investigación confirma la vigencia de los principios fundamentales de la soberanía digital: la documentación técnica exhaustiva como único escudo contra la opacidad algorítmica, la transparencia de telemetría como denuncia de la exfiltración de datos y el rastreo biométrico injustificado, y la identidad inalienable del legado digital como extensión del libre albedrío (Bentancor, n.d.).

El estudio permite formular las siguientes conclusiones:

La estandarización metodológica es viable. La triple hash, la validación de firmas digitales y el triage de permisos constituyen protocolos replicables que garantizan la integridad de la evidencia sin comprometer la privacidad del sujeto de datos (Bentancor, n.d.; “EL CÁNCER DE LA MEMORIA Y LA RESISTENCIA DIGITAL,” 2024).

El GDPR ofrece herramientas efectivas, aunque insuficientemente ejercidas. Los Art. 5, 15, 22, 3 y 83 conforman un arsenal normativo cuyo potencial depende de la capacidad técnica del titular para documentar la infracción (Bentancor, n.d.; “Gmail - ICO REFERRAL - Criminal Evidence ticket #2691688 - Roberto + Melisa - 24H DEADLINE.PDF,” n.d.).

La asimetría informativa es el núcleo del problema. Mientras las arquitecturas de telemetría oculta (SDKs inyectados, fingerprinting, registros ocultos) permanezcan opacas, el consentimiento será estructuralmente viciado y la soberanía del usuario, nominal (“EL CÁNCER DE LA MEMORIA Y LA RESISTENCIA DIGITAL,” 2024).

La inteligencia artificial puede operar como igualador asimétrico. Cuando una corporación se esconde tras un algoritmo, la voluntad del usuario y la precisión de las herramientas de análisis permiten documentar lo que la opacidad pretende ocultar (“El Cáncer de la Memoria: La Autopsia del Caballo de Troya y la Batalla por la Soberanía Digital,” 2026; “EL CÁNCER DE LA MEMORIA Y LA RESISTENCIA DIGITAL,” 2024).

Recomendaciones institucionales:

Establecer guías de auditoría forense móvil que integren el triage de permisos y la verificación de integridad como estándares mínimos para peritos y autoridades de control.

Promover la exigibilidad del acceso al DPO y la revisión humana de decisiones automatizadas como mecanismos de garantía de la soberanía digital.

Crear repositorios de jurisprudencia técnica (precedentes documentados) que orienten a los titulares de datos en la defensa de su legado digital.

Exigir transparencia efectiva en las transferencias internacionales, con evaluación de impacto cuando los datos fluyan hacia proveedores extracomunitarios (Bentancor, n.d.).

En definitiva, esta propuesta plantea una agenda de investigación que concilia el rigor

técnico del análisis forense con la tutela de los derechos fundamentales, demostrando que la auditoría de aplicaciones APK y registros de actividad no solo es compatible con el GDPR, sino que constituye su condición de posibilidad práctica: el peritaje forense como mecanismo de transparencia, y no como instrumento adicional de vigilancia.